IN THE CLAIMS:

Amended claims follow:

1.   (Cancelled)

2.   (Previously Amended) A computer program product as claimed in claim 4, wherein said sequence of predefined actions is user defined.

3.   (Previously Amended) A computer program product as claimed in claim 4, wherein one or more of said predefined actions is performed after receipt of a user input confirming said predefined action.

4.   (Currently Amended) A computer program product embodied on a computer readable medium for responding to detection of an outbreak of a computer virus on a computer apparatus, said computer program product comprising:

(i)   sequence data defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

(ii)   outbreak detection code operable to detect said outbreak; and

(iii)   sequence following code operable to follow said sequence of predefined actions;

wherein said sequence of predefined actions varies in dependence upon time of day.

5.   (Currently Amended) A computer program product embodied on a computer readable medium for responding to detection of an outbreak of a computer virus on a computer apparatus, said computer program product comprising:

(i)   sequence data defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

(ii)   outbreak detection code operable to detect said outbreak; and

(iii)   sequence following code operable to follow said sequence of predefined actions;

wherein said sequence of predefined actions varies in dependence upon day of week.

6.   (Previously Amended) A computer program product as claimed in claim 4, wherein one of said predefined actions is reducing virus detection notifications.

7.   (Previously Amended) A computer program product as claimed in claim 4, wherein one of said predefined actions is switching from virus quarantining to virus deletion when a computer virus is detected.

8.   (Previously Amended) A computer program product as claimed in claim 4, wherein one of said predefined actions is increasing scan options that control how thoroughly said computer system is scanned to detect a computer virus.

9.   (Previously Amended) A computer program product as claimed in claim 4, wherein one of said predefined actions is sending a copy of said detected computer virus to a remote site for analysis.

10.   (Previously Amended) A computer program product as claimed in claim 4, wherein one of said predefined actions is downloading a latest virus definition file from a remote site.

11.   (Previously Amended) A computer program product as claimed in claim 4, wherein one of said predefined actions is downloading a latest virus definition file from a remote site.

12.   (Previously Amended) A computer program product as claimed in claim 4, wherein one of said predefined actions is performing a complete virus scan of all computer files stored in at least a portion of said computer apparatus.

13.   (Cancelled)

14.   (Currently Amended) A computer program product embodied on a computer readable medium for responding to detection of an outbreak of a computer virus on a computer apparatus, said computer program product comprising:

(i)   sequence data defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

(ii)   outbreak detection code operable to detect said outbreak; and

(iii)   sequence following code operable to follow said sequence of predefined actions;

        wherein one of said predefined actions is blocking e-mail attachments;

        wherein said predefined action of blocking e-mail attachments blocks identical attachments appearing in excess of a threshold level.

15.   (Currently Amended) A computer program product embodied on a computer readable medium for responding to detection of an outbreak of a computer virus on a computer apparatus, said computer program product comprising:

(i)   sequence data defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

(ii)   outbreak detection code operable to detect said outbreak; and

(iii)   sequence following code operable to follow said sequence of predefined actions;

        wherein one of said predefined actions is rendering non-accessible e-mail distribution lists and e-mail address books of e-mail clients coupled to said computer apparatus.

16.   (Currently Amended) A computer program product embodied on a computer readable medium for responding to detection of an outbreak of a computer virus on a computer apparatus, said computer program product comprising:

(i)   sequence data defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

(ii)   outbreak detection code operable to detect said outbreak; and

(iii)   sequence following code operable to follow said sequence of predefined actions;

        wherein one of said predefined actions is restarting in administrator mode an e-mail post office coupled to said computer apparatus.

17.   (Currently Amended) A computer program product embodied on a computer readable medium for responding to detection of an outbreak of a computer virus on a computer apparatus, said computer program product comprising:

(i)   sequence data defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

(ii)   outbreak detection code operable to detect said outbreak; and

(iii)   sequence following code operable to follow said sequence of predefined actions;

wherein one of said predefined actions is closing down an e-mail post office coupled to said computer apparatus.

18.   (Cancelled)

19.   (Currently Amended) A method as claimed in claim 21, A method of responding to detection of an outbreak of a computer virus on a computer apparatus, said method comprising:

(i)   defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

(ii)   detecting said outbreak; and

(iii)   following said sequence of predefined actions;

wherein said sequence of predefined actions varies in dependence upon time of day;

wherein said sequence of predefined actions is user defined.

20.   (Currently Amended) A method as claimed in claim 21, A method of responding to detection of an outbreak of a computer virus on a computer apparatus, said method comprising:

(i)   defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

(ii)   detecting said outbreak; and

(iii)   following said sequence of predefined actions;

wherein said sequence of predefined actions varies in dependence upon time of day;

wherein one or more of said predefined actions is performed after receipt of a user input confirming said predefined action.

21. – 22. (Cancelled)

23.   (Currently Amended) A method as claimed in claim 21, A method of responding to detection

of an outbreak of a computer virus on a computer apparatus, said method comprising:

(i)   defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

(ii)   detecting said outbreak; and

(iii)   following said sequence of predefined actions;

      wherein said sequence of predefined actions varies in dependence upon time of day;

      wherein one of said predefined actions is reducing virus detection notifications.

24.   (Currently Amended) ~~A method as claimed in claim 21,~~ A method of responding to detection of an outbreak of a computer virus on a computer apparatus, said method comprising:

(i)   defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

(ii)   detecting said outbreak; and

(iii)   following said sequence of predefined actions;

      wherein said sequence of predefined actions varies in dependence upon time of day;

      wherein one of said predefined actions is switching from virus quarantining to virus deletion when a computer virus is detected.

25.   (Currently Amended) ~~A method as claimed in claim 21,~~ A method of responding to detection of an outbreak of a computer virus on a computer apparatus, said method comprising:

(i)   defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

(ii)   detecting said outbreak; and

(iii)   following said sequence of predefined actions;

      wherein said sequence of predefined actions varies in dependence upon time of day;

      wherein one of said predefined actions is increasing scan options that control how thoroughly said computer system is scanned
to detect a computer virus.

26.   (Currently Amended) ~~A method as claimed in claim 21,~~ A method of responding to detection of an outbreak of a computer virus on a computer apparatus, said method comprising:

(i)   defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

(ii)   detecting said outbreak; and

(iii)   following said sequence of predefined actions;

        wherein said sequence of predefined actions varies in dependence upon time of day;

        wherein one of said predefined actions is sending a copy of said detected computer virus to a remote site for analysis.

27.   (Currently Amended) ~~A method as claimed in claim 21,~~ A method of responding to detection of an outbreak of a computer virus on a computer apparatus, said method comprising:

(i)   defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

(ii)   detecting said outbreak; and

(iii)   following said sequence of predefined actions;

        wherein said sequence of predefined actions varies in dependence upon time of day;

        wherein one of said predefined actions is downloading a latest virus definition file from a remote site.

28.   (Cancelled)

29.   (Currently Amended) ~~A method as claimed in claim 21,~~ A method of responding to detection of an outbreak of a computer virus on a computer apparatus, said method comprising:

(i)   defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

(ii)   detecting said outbreak; and

(iii)   following said sequence of predefined actions;

        wherein said sequence of predefined actions varies in dependence upon time of day;

        wherein one of said predefined actions is performing a complete virus scan of all computer files stored in at least a portion of said computer apparatus.

30.   (Cancelled)

31.   (Previously Amended) A method of responding to detection of an outbreak of a computer virus on a computer apparatus, said method comprising:

(i)   defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

(ii)   detecting said outbreak; and

(iii)   following said sequence of predefined actions;

wherein one of said predefined actions is blocking e-mail attachments;

wherein said predefined action of blocking e-mail attachments blocks identical attachments appearing in excess of a threshold level.

32.   (Previously Amended) A method of responding to detection of an outbreak of a computer virus on a computer apparatus, said method comprising:

(i)   defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

(ii)   detecting said outbreak; and

(iii)   following said sequence of predefined actions;

wherein one of said predefined actions is rendering non-accessible e-mail distribution lists and e-mail address books of e-mail clients coupled to said computer apparatus.

33.   (Previously Amended) A method of responding to detection of an outbreak of a computer virus on a computer apparatus, said method comprising:

(i)   defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

(ii)   detecting said outbreak; and

(iii)   following said sequence of predefined actions;

wherein one of said predefined actions is restarting in administrator mode an e-mail post office coupled to said computer apparatus.

34.   (Previously Amended) A method of responding to detection of an outbreak of a computer virus on a computer apparatus, said method comprising:

(i)   defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

(ii)   detecting said outbreak; and

(iii)   following said sequence of predefined actions;

wherein one of said predefined actions is closing down an e-mail post office coupled to said computer apparatus.

35.   (Cancelled)

36.   (Previously Amended) A computer program product as claimed in claim 38, wherein said sequence of predefined actions is user defined.

37.   (Previously Amended) A computer program product as claimed in claim 38, wherein one or more of said predefined actions is performed after receipt of a user input confirming said predefined action.

38.   (Currently Amended) ~~Apparatus~~ A system including a computer program product embodied on a computer readable medium for responding to detection of an outbreak of a computer virus on a computer apparatus, said computer program product comprising:

sequence data storage storing sequence data defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

outbreak detection logic operable to detect said outbreak; and

sequence following logic operable to follow said sequence of predefined actions;

wherein said sequence of predefined actions varies in dependence upon time of day.

39.   (Currently Amended) ~~Apparatus~~ A system including a computer program product embodied on a computer readable medium for responding to detection of an outbreak of a computer virus on a computer apparatus, said computer program product comprising:

sequence data storage storing sequence data defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

outbreak detection logic operable to detect said outbreak; and

sequence following logic operable to follow said sequence of predefined actions;

wherein said sequence of predefined actions varies in dependence upon day of week.

40.   (Previously Amended) A computer program product as claimed in claim 38, wherein one of said predefined actions is reducing virus detection notifications.

41.   (Previously Amended) A computer program product as claimed in claim 38, wherein one of said predefined actions is switching from virus quarantining to virus deletion when computer virus is detected.

42.   (Previously Amended) A computer program product as claimed in claim 38, wherein one of said predefined actions is increasing scan options that control how thoroughly said computer system is scanned to detect a computer virus.

43.   (Previously Amended) A computer program product as claimed in claim 38, wherein one of said predefined actions is sending a copy of said detected computer virus to a remote site for analysis.

44.   (Previously Amended) A computer program product as claimed in claim 38, wherein one of said predefined actions is downloading a latest virus definition file from a remote site.

45.   (Previously Amended) A computer program product as claimed in claim 38, wherein one of said predefined actions is downloading a latest virus definition file from a remote site.

46.   (Previously Amended) A computer program product as claimed in claim 38, wherein one of said predefined actions is performing a complete virus scan of all computer files stored in at least a portion of said computer apparatus.

47.   (Cancelled)

48.   (Currently Amended) ~~Apparatus~~ <u>A system including a computer program product embodied</u>

on a computer readable medium for responding to detection of an outbreak of a computer virus on a computer apparatus, said computer program product comprising:

sequence data storage storing sequence data defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

outbreak detection logic operable to detect said outbreak; and

sequence following logic operable to follow said sequence of predefined actions;

wherein one of said predefined actions is blocking e-mail attachments;

wherein a said predefined action of blocking e-mail attachments blocks identical attachments appearing in excess of a threshold level.

49.   (Currently Amended) ~~Apparatus~~ A system including a computer program product embodied on a computer readable medium for responding to detection of an outbreak of a computer virus on a computer apparatus, said computer program product comprising:

sequence data storage storing sequence data defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

outbreak detection logic operable to detect said outbreak; and

sequence following logic operable to follow said sequence of predefined actions;

wherein one of said predefined actions is rendering non-accessible e-mail distribution lists and e-mail address books of e-mail clients coupled to said computer apparatus.

50.   (Currently Amended) ~~Apparatus~~ A system including a computer program product embodied on a computer readable medium for responding to detection of an outbreak of a computer virus on a computer apparatus, said computer program product comprising:

sequence data storage storing sequence data defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

outbreak detection logic operable to detect said outbreak; and

sequence following logic operable to follow said sequence of predefined actions;

wherein one of said predefined actions is restarting in administrator mode an e-mail post office coupled to said computer apparatus.

51.   (Currently Amended) ~~Apparatus~~ A system including a computer program product embodied

on a computer readable medium for responding to detection of an outbreak of a computer virus on a computer apparatus, said computer program product comprising:

sequence data storage storing sequence data defining a sequence containing a plurality of predefined actions to be followed upon detection of said outbreak;

outbreak detection logic operable to detect said outbreak; and

sequence following logic operable to follow said sequence of predefined actions;

wherein one of said predefined actions is closing down an e-mail post office coupled to said computer apparatus.